

## WHAT IS CLAIMED IS:

*Sub are*

1. A parallel counter comprising:  
 a plurality of inputs for receiving a binary number as a plurality of binary inputs;  
 a plurality of outputs for outputting binary code indicating the number of binary ones in the plurality of binary inputs; and  
 a logic circuit connected between the plurality of inputs and the plurality of binary outputs and for generating each of the plurality of binary outputs as a symmetric function of the binary inputs. *? (1)*

*Fig. 11*

2. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate at least one of the binary outputs as a symmetric function of the binary inputs using exclusive OR logic for combining a plurality of sets of one or more binary inputs.

*Fig. 9*  
*but not part of parallel counter*

3. A parallel counter according to claim 2 wherein said logic circuit is arranged to logically AND members of each set of binary inputs and to logically exclusively OR the result of the AND operations.

*Fig. 9*  
*but not part of parallel counter*

4. A parallel counter according to claim 3 wherein said logic circuit is arranged to logically AND  $2^i$  of the binary inputs in each set for the generation of the  $i^{\text{th}}$  binary output, where  $i$  is an integer from 1 to  $N$ ,  $N$  is the number of binary outputs and  $i$  represents the significance of each binary output, each set being unique and the sets covering all possible combinations of binary inputs.

5. A parallel counter according to claim 3 wherein said logic circuit is arranged to logically AND members of each set of binary inputs, where each set is unique and the sets cover all possible combinations of binary inputs.

6. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate at least one of the binary outputs as a symmetric function of the binary inputs using OR logic for combining a plurality of sets of one or more binary inputs.

*(12) min - design  
 Where is Dwg.?*

*(12)  
 3-5  
 x  
 3-5  
 9*

Sub 2

Sub  
a2

9. ~~A parallel counter according to claim 7 wherein said logic circuit is arranged to logically AND members of each set of binary inputs, where each set is unique and the sets cover all possible combinations of binary inputs.~~

10. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate a first binary output as a symmetric function of the binary inputs using exclusive OR logic for combining a plurality of sets of one or more binary inputs, and to generate an N<sup>th</sup> binary output as a symmetric function of the binary inputs using OR logic for combining a plurality of sets of one or more binary inputs.

11. A parallel counter according to claim 1 wherein said logic circuit is arranged to generate two possible binary outputs for a binary output less significant than the  $N^{\text{th}}$  binary output, as symmetric functions of the binary inputs using OR logic for combining a plurality of sets of one or more binary inputs where N is the number of binary outputs, the sets used for each possible binary output being of two different sizes which are a function of the binary output being generated; and said logic circuit including selector logic to select one of the possible binary outputs based on a more significant binary output value.

Subh  
a2

14. ~~A parallel counter according to claim 13 wherein said subcircuit logic modules are arranged to use OR logic for combining sets of said some of said binary inputs.~~

16. A logic circuit for multiplying two  $N$  bit binary numbers, the logic circuit comprising:

5 trays  
702, 704,  
706

Fig. 17  
top  
+ Fig. 18

5 tubes and  
308  
enclosed  
for CPA

12)  
min - less  
cryption  
e.g. A, B,  
not guaranteed  
two parties  
e.g. 15

17. A logic circuit according to claim 16 wherein said array generation logic is arranged to perform the further logical combination of values for values formed by the logical AND combination of each bit  $A_i$  of one binary number and each bit  $B_j$  of the other binary number, where  $i-j-k \leq 1$ ,  $k$  is a chosen integer, and  $i$  and  $j$  are integers from 1 to  $N$ .

18. A logic circuit according to claim 16 wherein said array generation logic is arranged to logically AND combine each bit  $A_i$  of the first binary number with each bit  $B_j$  of a second binary number to generate said array comprising a sequence of binary numbers represented by said logical AND combinations,  $A_i$  AND  $B_j$  and to carry out further logical combination by logically combining the combination  $A_1$  AND  $B_{N-2}$ ,  $A_1$  AND  $B_{N-1}$  where  $N$  is the number of bits in the binary numbers.

19. A logic circuit according to claim 18 wherein said array generation logic is arranged to combine the combinations  $A_1$  AND  $B_{N-2}$  and  $A_0$  AND  $B_{N-1}$ , using exclusive OR logic to replace these combinations, and to combine  $A_1$  AND  $B_{N-1}$  and  $A_0$  AND  $B_{N-2}$  to replace the  $A_1$  AND  $B_{N-1}$  combination.)

20. A logic circuit according to claim 16 wherein said array reduction logic includes at least one of: at least one full adder, at least one half adder, and at least one parallel counter.

21. A logic circuit according to claim 20 wherein said array reduction logic includes at least one parallel counter according to any one of claims 1 to 15.